Коды Голея и системы Штайнера

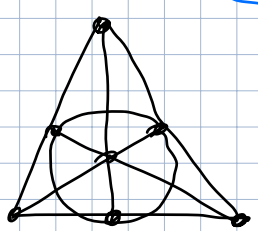
Определение. Система Штайнера $S(t, k, n)$

блоки

Семейство k-элементных подмножеств n-элементного мн-ва S_n такое, что $\forall$ t-элементное под-во в S_n содержится ровно в одном k-элементном блоке мн-ва.

Пример. $S(2, 3, 7)$ = Плоскость Фано

$\mathbb{P}^2(\mathbb{F}_2)$ -- $\mathbb{F}_2^3$



каждая пр. прямая сод. 3 точки, прямых 7

Через любые две точки проходит ед. пр. прямая.

Цель: увидеть, что G_{23}, G_{24} дают системы Штайнера типов

$S(4, 7, 23)$ $S(5, 8, 24)$

Напоминание.

Теорема (доказана).

1) Код Голея G_{23} есть совершенный бинарный код типа $[23, 12; 7]$

$G_{23} \subset \mathbb{F}_2^{23}$, $\dim G_{23} = 12$, $d(G_{23}) = 7$.

2) Чётное расширение $G_{24} = \overline{G_{23}}$ самодвойственный код типа $[24, 12; 8]$

$G_{24}^{\perp} = G_{24}$.

Исследуем комбинаторику стр. G_{23}.

$$G_{23} = C_{e_+(x)} = C_{f_+(x)}$$

$$e_+(x) = \sum_{\left(\frac{k}{23}\right)=1} x^k = x^1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}.$$

Порожд. матрица $G = M_{12\times 23}(\mathbb{F}_2)$ – строится из цикл. перестановок вектора $e_+(x)$, $W(e_+(x)) = 11$.

$f_+(x) = \text{нод}(e_+(x), x^{23} - 1) =$

$= 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ (3)

$w(f_1(x)) = 7$

$\overline{f_1(x)} \in G_{24} \Rightarrow w(\overline{f_1(x)}) = 8$ — нечетный.

Вывод: G_{24} — порождается нечетными или $(\overline{f_1(x)})$ четным.

$G_{24} \to G_{12\times 24}$ (нечетная / четная) $\to [(G' | E_{12})]$

$G' \in M_{12\times 12}(\mathbb{F}_2)$

Теорема 2 (Распределение слов в G_{23}, G_{24})

G_{23}

Вес	0	7	8	11	12	15	16	23
#	1	253	506	1288	1288	506	253	1

G_{24}

нечетный $S(5,8,24)$

Вес	0	8	12	16	24
#	1	759	2576	759	1

Д-во (1) $\mathbb{1} = (1,\dots,1) \in G_{23}$

$\underline{1\!\!1} = \underbrace{1 + x + \ldots + x^{p-1}} \in G_{23} = G_{f_+(x)}$ (4)

$x^p - 1 = (x-1)\underbrace{f_+(x)}_{\text{св. вектор}} \underbrace{f_-(x)}_{\text{св. не вектор}}$

$f_I(x) = \prod_{(\frac{k}{p})=\pm 1} (x - \alpha^k) \quad C_{Q12}(p)$

$\frac{x^p-1}{x-1} = f_-(x) f_+(x) \in C_{f_+(x)}$

Симметрия в задаче 1.

$w(u) = t \quad w(u + \underline{1\!\!1}) = 23 - t \quad (G_{23})$

$w(u) = t \quad w(u + \underline{1\!\!1}_{24}) = 24 - t \quad (G_{24})$

Найдём $N_7^{(23)} = ?$ (код совершенный!)

$F_2^{23} = \bigsqcup_{u \in G_{23}} B_3(u)$

Рассмотрим произвольный вектор $u_4 \in F_2^{23}$ веса $w(u_4) = 4$.

$\exists!\ u \in G_{23} : u_4 \in B_3(u),\ w(u) = k.$

$3 \geqslant f(u_4, m) = w(u_4 + m) =$ общие единицы

$= 4 + k - 2|u_4 \wedge m|$ (5)

$4 \geqslant |u_4 \wedge m| \geqslant \frac{k+1}{2} \Rightarrow 7 \geqslant k \Rightarrow \boxed{k = 7}$

Более того, в этом случае $|u_4 \wedge m_7| = 4$

$4 \geqslant |u_4 \wedge m| \geqslant 4 \Rightarrow \boxed{u_4 \subset m_7.}$

Факт: $\forall\ u_4 \in \mathbb{F}_2^{23}\ \exists!\ m_7 \in G_{23}$:

$u_4 \subset m_7.$

$\{m_7 \in G_{23}\}$ образуют систему

Штейнера $S(4, 7, 23)$.

$N_7^{(23)} = ?$ 253 - блока по 7 элементов

$u_4 \in \mathbb{F}_2^{23}$ → 4 некулевых координаты →

4-эл. множество числа $\{1, 2, \ldots, 23\}$

Всего у нас C_{23}^4 - таких подмножеств

$C_7^4 \cdot N_7^{(23)} = C_{23}^4$

$N_7^{(23)} = \frac{23 \cdot 22 \cdot 21 \cdot 20}{7 \cdot 6 \cdot 5 \cdot 4} = 23 \cdot 11 = 230 + 23 = 253$

(6)

$N_8^{(23)} = ?$

$u_5 \in \mathbb{F}_2^{23} \Rightarrow \exists\, m_k \in G_{23} \quad u_5 \in B_3(m_k)$

$3 \geq \delta(u_5, m_k) = 5 + k - 2|u_5 \wedge m_k|$

$5 \geq |u_5 \wedge m_k| \geq \frac{k+2}{2} \Rightarrow k = 7, 8 \Rightarrow$

$u_5 \subset m_7, m_8.$

$C_{23}^5 = N_7^{(23)} C_7^5 + N_8^{(23)} \cdot C_8^5 \Rightarrow$

$\#\{u_5\}$

$\boxed{N_8^{(23)} = 506}$

Почему нет других слов:

$C_{24}^1 = G_{24} \Rightarrow \forall\, m \in G_{24} \quad w(m) \equiv 0\,(4)$

$G_{24} = \overline{G_{23}} \quad w(G_{23}) \geq 7$

$w(m) = 7, 8, 9, 10, 11, 12 \Rightarrow$ слова G_{23}

симметрия.

$23 - 7, -8, -11, 12.$

Упражнение. Окладу в G_{24} образуют систему Штайнера $S(5, 8, 24)$.

Информация Совершенных кодов

Известно, что все совершенные (не обязательно линейные) коды распадаются на 4 класса:

1) Тривиальные ($\overline{0}$, $\overline{1}$, простейшие повторяющиеся).

2) Код Хэмминга над F_q. $d=3$

3) $G_{23} = [23, 12; 7]_{F_2}$.

4) $G_{11} = [11, 6; 5]_{F_3}$. → Пример на второй семестр

Лекция в понедельник:

$C_{QR}(p) \longrightarrow SL_2(F_p)$

координаты можно закодировать элементами из F_p

Упражнение. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \iff$ (8)

2 кв. вычет $\bmod p \iff p \equiv \pm 1 \ (8)$

невычет $\iff p \equiv \pm 3 \ (8)$

Указание:

$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \bmod p.$

$\boxed{2 = (\alpha + \alpha^{-1})^2}$ $\quad \alpha^8 = 1 \bmod p.$

$\forall\ p \neq 2 \quad p^2 \equiv 1 \bmod 8 \Rightarrow \alpha \in \mathbb{F}_{p^2}$

$2^{\frac{p-1}{2}} = (\alpha + \alpha^{-1})^{p-1} = \frac{(\alpha + \alpha^{-1})^p}{(\alpha + \alpha^{-1})} \overset{\mathbb{F}_p}{=}$

$= \frac{\alpha^p + \alpha^{-p}}{\alpha + \alpha^{-1}} \quad \begin{matrix} p = \pm 1 \ (8) \\ = \\ p = \pm 3 \ (8) \end{matrix} \quad ?$
